

--	--	--	--	--	--	--	--	--	--

# MULTIMEDIA UNIVERSITY

## FINAL EXAMINATION

TRIMESTER 1, 2015/2016

### **TNS3131 – NETWORK SECURITY AND MANAGEMENT** (All Sections / Groups)

5 OCTOBER 2015  
2.30 p.m. – 4.30 p.m.  
(2 Hours)

---

#### INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 printed pages including cover page with 6 questions only.
2. Attempt **ALL** questions in Section A and attempt **ONE** out of **TWO** questions in Section B. Marks and the distribution of marks for each question is given.
3. Please write all your answer in the Answer Booklet provided.

**Section A: Attempt ALL questions****Question 1 [10 Marks]**

(a) Briefly define the following components of OSI security architecture.

- i) Security attack
- ii) Security mechanism
- iii) Security service

[3 Marks]

(b) With an aid of diagram, describe **FOUR** basic tasks in designing a security service.

[5 Marks]

(c) What is the difference between reactive and proactive network management?

[2 Marks]

**Question 2 [10 Marks]**

(a) What are the **FOUR** principal services provided by PGP?

[2 Marks]

(b) What is the difference between IPSec transport mode and tunnel mode?

[2 Marks]

(c) What are the key elements of the Simple Network Management Protocol (SNMP) model?

[2 Marks]

(d) Which factors of wireless networks are of higher security risk compared to wired network?

[4 Marks]

**Question 3 [10 Marks]**

(a) List **TWO** classes of intruders.

[2 Marks]

(b) What are **TWO** common techniques used to protect a password file?

[2 Marks]

(c) Explain **THREE** general techniques used in a firewall.

[6 Marks]

**Continued ...**

**Question 4 [10 Marks]**

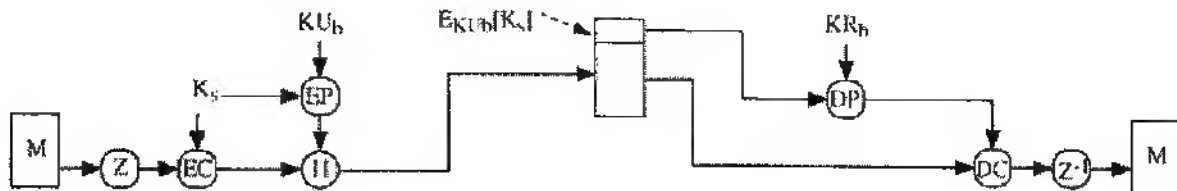
- (a) What are the **TWO** basic functions used in encryption algorithms? [2 Marks]
- (b) List and briefly define **THREE** uses of a public-key cryptosystem. [6 Marks]
- (c) What is the purpose of the X.509 standard? [2 Marks]

Continued ...

**Section B: Attempt ONE out of TWO questions.**

**Question 5 [20 Marks]**

- (a) With the aid of diagram below, identify the PGP service and describe the sequence of operations of that service.



$K_s$	= session key used in conventional encryption scheme
$KR_b$	= private key of user A, used in public-key encryption scheme
$KU_a$	= public key of user A, used in public-key encryption scheme
EP	= public-key encryption
DP	= public-key decryption
EC	= conventional encryption
DC	= conventional decryption
H	= hash function
	= concatenation
Z	= compression using ZIP algorithm

[6 Marks]

- (b) How is IPSec important for internetworking routing? [4 Marks]
- (c) What is the difference between an SSL connection and an SSL session? [2 Marks]
- (d) What is the relationship among SNMPv1, SNMPv2 and SNMPv3? [3 Marks]
- (e) Explain the **FIVE** different phases of operation of an IEEE802.11i Robust Security Network (RSN). [5 Marks]

**Continued ...**

**Question 6 [20 Marks]**

- (a) With aid of diagrams, describe the encryption and decryption of triple DES.  
[8 Marks]
- (b) Describe Diffie-Hellman key exchange.  
[8 Marks]
- (c) i) What is Kerberos?  
ii) What problem was Kerberos designed to address?  
[4 Marks]

**End of Page**

